



Présentation du Projet : Dingo Lingo

Groupe D Réseaux d'Entreprise

3 Février 2026

Table des matières

1 Présentation projet	4
2 Objectifs	4
3 Notre société	4
3.1 Les employés	5
3.2 Responsabilité spécifique	5
4 Contact et encadrement	6
5 Charte d'Équipe - Groupe D (DingoLingo)	7
6 TimeSheets & Suivi	7
6.1 Outil de Gestion : Clockify	7
6.2 Directives de Saisie	7
6.3 Suivi Individuel	8
6.4 Temps de travail total de l'équipe	8
7 Journal de Bord : Lundi 02	9
7.1 10h00 Réunion de lancement : Organisation	9
7.2 14h30 État des lieux technique et infrastructure	9
7.3 15h30 Réunion de suivi avec M. Schalkwijk	9
7.4 16h17 Bilan de fin de journée	9
7.5 17h00 Réunion inter-groupes (Groupe C)	10
7.6 Résumé de la journée en quelques photos	10
8 Journal de Bord : Mardi 03	11
8.1 09h00 Réunion du matin : Organisation	11
8.2 État de l'avancement avant la pause midi	11
8.3 Team Building - Pizza Party	12
8.4 16h30 Réunion du soir : Résumé de la journée	12
8.5 Résumé de la journée en quelques photos	12
9 Journal de Bord : Mercredi 04	13
9.1 09h00 Réunion du matin : Organisation	13
9.2 16h00 Réunion du soir : Résumé de la journée	14
9.3 Résumé de la journée en quelques photos	14
10 Journal de Bord : Jeudi 05 (En cours)	14
10.1 09h00 Réunion du matin : Organisation	14
10.2 [16H30] Réunion du soir : Résumé de la journée	15
10.3 Résumé de la journée en quelques photos	16
11 Topologie et plan d'adressage	17
11.1 Topologie logique	17
11.2 VLAN et plans d'adressage	17
11.2.1 Tableau des VLAN	17
11.2.2 Adresses statiques	17
11.3 Topologie physique	18

12 Configuration Firewall & VPN	20
12.1 Flux théoriques	20
12.1.1 1. Interface : WAN	20
12.1.2 2. Interfaces : IT (VLAN 10) & EMP (VLAN 20)	20
12.1.3 3. Interface : DMZ (VLAN 80)	20
12.1.4 4. Interface : MONIT (VLAN 60)	21
12.1.5 5. Interface : AD (VLAN 70)	21
12.1.6 6. Interface : ADMIN (VLAN 100)	21
12.2 Règles implémentées (Captures d'écran)	22
13 Sécurité	25
14 Sécurisation des Commutateurs (Switching)	25
14.1 Durcissement global et administratif	25
14.2 Protection contre les attaques DHCP (DHCP Snooping)	25
14.3 Protection contre l'ARP Poisoning (DAI)	26
14.4 Protection de l'architecture VLAN (DTP & Hopping)	26
14.5 Protection STP et Port Security	26
14.6 Durcissement des équipements (Device Hardening)	27
14.7 Sécurité de Niveau 2 (Switching)	27
15 LDAP et Authentification	28
15.1 Description du processus	28
16 Développement Web	29
16.1 Architecture Logicielle : Full-Stack Next.js & Prisma	29
16.2 1. Infrastructure & Virtualisation	29
16.3 2. Développement Backend & Base de Données	29
16.4 3. Sécurité & Authentification (LDAP)	29
16.5 État du service LDAP	29
16.6 4. Architecture du projet	32
17 Reverse Proxy - Traefik	33
17.1 Objectif du reverse proxy	33
17.2 Architecture globale	33
17.3 Configuration de Traefik (Docker Compose)	33
17.4 Intégration de l'application Next.js	34
17.4.1 Routage et Middlewares de Sécurité	35
17.5 Gestion des certificats et Environnements	35
17.5.1 Workflow Let's Encrypt	35
17.5.2 Séparation Production / Développement	35
17.6 Résumé des bénéfices	36
18 Solution de Monitoring	37
18.1 Architecture retenue	37
18.2 Objets de monitoring	37
18.3 Objectifs fonctionnels	37
18.4 Avantages de cette solution	38
19 Solution de centralisation des logs	39
19.1 Architecture retenue	39
19.2 Objectifs fonctionnels	39
19.3 Avantages de cette solution	39

1 Présentation projet

Dans le cadre du cours **Réseaux d'entreprise**, nous sommes une équipe d'administrateurs réseaux et systèmes d'une entreprise dans les formations en ligne.

L'entreprise propose un portail en ligne qui inclut une liste des formateurs et des formations, organisées par thèmes, ainsi qu'une solution professionnelle pour le suivi des formations en ligne.

C'est une plateforme spécialisée dans les formations pour les langues.

Nous avons choisi **Dingo Lingo** comme nom.



FIGURE 1 – Logo Dingo Lingo

2 Objectifs

Notre mission est de fournir une infrastructure **haute disponibilité** et **sécurisée** pour notre portail de formation en ligne.

- **Conception** : Architecture réseau robuste et évolutive (Scaling).
- **Accessibilité** : Publication sécurisée des services (Web).
- **Sécurité** : Mise en œuvre de Firewalls, VPN inter-sites avec le Groupe C, et gestion rigoureuse des accès (RGPD).

3 Notre société

Groupe : D

Local : L218

Notre entreprise fait partie d'une multinationale. Nous devons être capables de communiquer avec la société **CrossTalk** (groupe C).

Note profs : Vous êtes libres de prendre toutes les initiatives que vous jugez pertinentes, et ce sont ces initiatives qui feront la différence.

3.1 Les employés

NOM	Prénom
AKTAMIROV	Khasan
BEN LHAJ	Rayane
DEVIS	Xavier
EL MAZANI	Mohamed Mokhtar
GÉRARD	Liam
HENRARD	Quentin
HOEDENAEKEN	Nicolas
MERTENS	Corentin
STÄRKEL	Arno
STOCQ	Martin
VANDERMEULEN	Yann
VIER	Clément
WILLEMS	Julien
ZEBIRI	Saâd

TABLE 1 – Liste des employés

Rôle	Employés
Coordinateur de Projet	Liam GÉRARD
Assistant coordinateur	Corentin MERTENS
Équipe sécurité	* Arno STÄRKEL Saâd ZEBIRI Martin STOCQ Khasan AKTAMIROV
Équipe administration	* Yann VANDERMEULEN Julien WILLEMS Quentin HENRARD Clément VIER Mohamed EL MAZANI Rayane BEN LHAJ
Équipe Web	Clément VIER Rayane BEN LHAJ Nicolas HOEDENAEKEN
Équipe monitoring	* Rayane BEN LHAJ

* : Responsable de l'équipe

3.2 Responsabilité spécifique

- **Responsable des rapports** : Nicolas HOEDENAEKEN
- **Responsable ressources informatiques** : Julien WILLEMS
- **Responsable communication inter-groupes** : Liam GÉRARD

- **Responsable timesheet** : Xavier DEVIS
- **Responsable état des lieux** : Quentin HENRARD
- **Responsable photos** : L'ensemble du groupe

4 Contact et encadrement

Liam GÉRARD (Coordinateur de Projet) : l.gerard@students.ephec.be

Corentin MERTENS (Assistant coordinateur) : c.mertens@students.ephec.be

Ce projet est principalement encadré par :

M. Schalkwijk : l.schalkwijk@ephec.be

Mme Vroman : mn.vroman@ephec.be

5 Charte d'Équipe - Groupe D (DingoLingo)

Le présent document a été établi lors de la réunion de lancement de ce **lundi 02 février 2026 à 10h00**. Il définit les principes de fonctionnement, les responsabilités et les règles de conduite que l'ensemble des membres du groupe s'engage à respecter durant toute la durée du projet.

L'objectif de cette charte est de garantir un environnement de travail productif, une communication transparente et une infrastructure réseau de haute qualité.

Document officiel : Consulter la Charte complète (PDF)

6 TimeSheets & Suivi

Cette page centralise le suivi du temps de travail de l'équipe **Groupe D**. L'objectif est d'assurer une transparence totale sur l'avancement des tâches et de garantir le respect des objectifs de productivité.

6.1 Outil de Gestion : [Clockify](#)

Nous utilisons **Clockify** pour le tracking en temps réel.

- **Workspace** : Projet Réseaux Groupe D
- [Lien d'accès](#)
- **Responsable du suivi** : Xavier DEVIS

6.2 Directives de Saisie

Pour assurer la cohérence des rapports, chaque membre doit respecter les conventions suivantes lors de la saisie de ses activités :



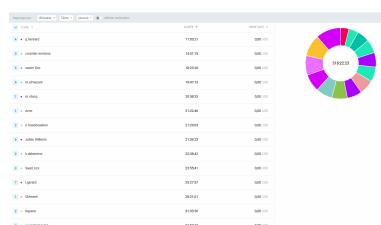
1. **Description** : Au lieu de "Travail réseau", préférez "Config VPN Inter-site avec Groupe C".
2. **Fréquence** : Saisie obligatoire à la fin de chaque session de travail (matin/après-midi).

6.3 Suivi Individuel

Membre	Rôle	Heures	Tâches Principales
Yann V.	Resp. Admin	37h	Infrastructure, LDAP
Rayane B.	Équipe Web	32h	Frontend, Backend, Reverse-Proxy
Clément V.	Équipe Admin	28h	Topologies, VPN
Liam G.	Coordinateur	26h	Management, Com Inter-groupe, Wiki
Saad K.	Équipe Sécu	24h	Firewall, L3
Khasan A.	Équipe Admin	23h	Config L2/L3, Vlans, ACL
Julien W.	Équipe Admin	22h	AD, VMs, Router
Arno S.	Resp. Sécurité	21h	Firewall, flux
Martin S.	Équipe Sécu	21h	Firewall, L2
Nicolas H.	Équipe Rapport	21h	Rapport, WEB
Mohamed E.	Équipe Admin	20h	Monitoring, VM, Déploiement
Xavier D.	Gestion Timesheet	18h	Suivi administratif, Admin
Corentin M.	Équipe Web	14h	WEB, Management
Quentin H.	Équipe Rapport	12h	Notes
TOTAL	Groupe D	319h	Investissement global

TABLE 2 – Récapitulatif des heures prestées par membre

6.4 Temps de travail total de l'équipe



7 Journal de Bord : Lundi 02

7.1 10h00 | Réunion de lancement : Organisation

Définition de la structure de l'entreprise et répartition des responsabilités.

Décisions

- Rédaction et validation de la Charte d'Équipe.
- Attribution des rôles de coordination et des pôles techniques (Sécurité, Administration, Web, Monitoring).
- Établissement des horaires de travail et des méthodes de communication.

7.2 14h30 | État des lieux technique et infrastructure

Analyse de l'existant physique et débats sur l'architecture.

Réalisations pratiques

- Accès internet opérationnel sur le routeur.
- Identification des deux serveurs physiques (Proxmox) : connectivité en cours de configuration.

Conception

- Schémas logique et physique en phase de finalisation (WIP).
- Lancement de la réflexion sur le Web.

Points de débat

Discussions sur le nombre de pare-feu (1 ou 2), le choix entre instances virtuelles ou physiques, et l'ajout éventuel de serveurs supplémentaires.

7.3 15h30 | Réunion de suivi avec M. Schalkwijk

Revue des schémas d'infrastructure et conseils techniques.

— Modifications apportées suite au feedback :

- Intégration d'une interface de gestion dédiée.
- Abandon de la solution en cluster pour simplifier l'architecture.
- Mise en place d'une zone DMZ.
- Sécurisation du serveur Web : mise en œuvre d'une authentification via un contrôleur de domaine (DC) en mode "Read-Only".
- Arbitrage Firewall : Liberté totale accordée sur le choix entre virtuel ou physique.

Les schémas ont été mis à jour immédiatement durant la session pour refléter ces changements.

7.4 16h17 | Bilan de fin de journée

Avancement par pôle

- **Administration Réseau** : Communication établie entre les deux serveurs Proxmox. Déploiement d'OPNsense en cours.
- **Web** : Développement de l'interface Front-End quasiment achevé.
- **Sécurité** : Validation finale des schémas de sécurité.

- **Documentation** : Wiki structuré et mise à jour des rapports en cours.

Objectifs prioritaires (Prochaines étapes)

- Établissement de la Roadmap détaillée de la semaine.
- Développement du Back-End pour le portail Web.
- Configuration des flux et des règles de filtrage sur le Firewall.
- Mise en place d'un VLAN temporaire unique pour faciliter le travail collaboratif initial avant segmentation.

7.5 17h00 | Réunion inter-groupes (Groupe C)

Alignement des infrastructures et définition des objectifs d'interconnexion avec la société CrossTalk (groupe C).

Synthèse des échanges

- Présentation de l'avancement du Groupe D (basée sur la réunion de 16h).
- **Étude comparative avec les choix techniques du Groupe C :**
 - *Monitoring* : Ils ont opté pour la suite LibreNMS couplée à un serveur Syslog.
 - *Infrastructure* : Leur schéma physique est validé, le schéma logique est en cours de finalisation.
 - *Sécurité* : Utilisation confirmée de la solution pfSense comme Firewall principal.

Objectif commun déterminé

- Mise en place d'un tunnel VPN Site-to-Site pour permettre la communication sécurisée entre les deux infrastructures.
- **Échéance fixée** : Opérationnalité complète attendue pour le mercredi 04 février.

7.6 Résumé de la journée en quelques photos

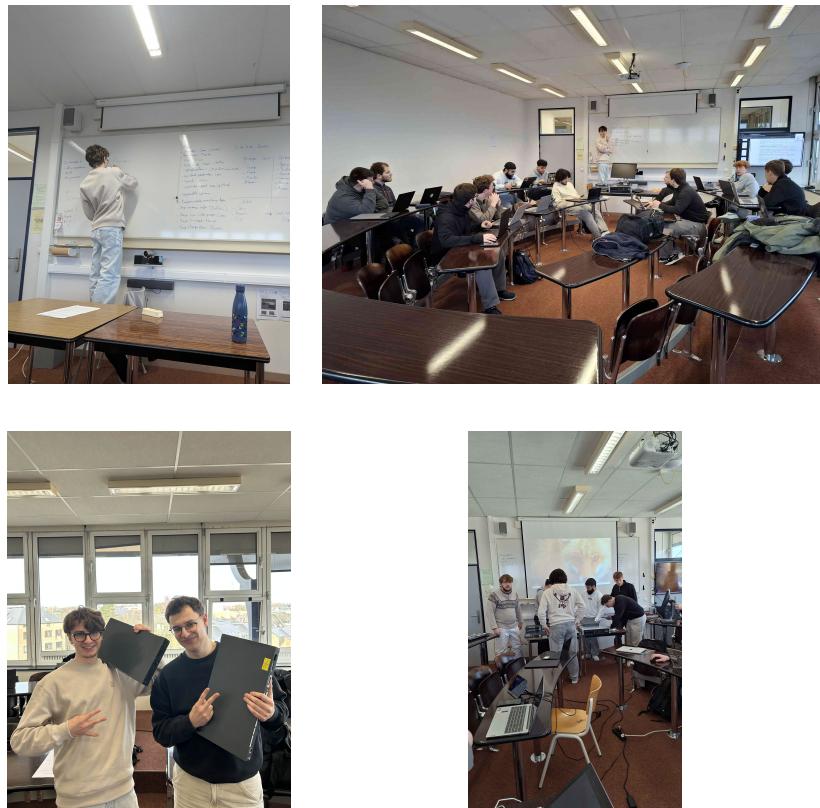


FIGURE 2 – Installation physique et configuration initiale

8 Journal de Bord : Mardi 03

8.1 09h00 | Réunion du matin : Organisation

Mise au point de l'avancement du travail, établissement des objectifs journaliers et répartition des tâches.

Objectifs journaliers

- Choix du logo.
- Création des diagrammes de flux et de règles.
- Installation du firewall.
- Réflexion et création de l'Active Directory.
- Analyse technique pour l'installation du VPN.
- Création du Backend.

Questions soulevées

- Quid des nouveaux schémas ?
- Que mettre en place au niveau du Backend ?

8.2 État de l'avancement avant la pause midi

Plusieurs étapes clés ont pu être complétées durant la matinée :

- Connexion SSH établie sur le routeur.
- Plan des flux et règles firewall bien avancé.
- Installation de Proxmox complétée.

- Création de containers Docker.
- Installation de pfSense.

Problèmes rencontrés

- **DNS** : Problème avec le nom de domaine (non validé par OVH).
- **Réseau** : Pas de connexion internet sur le LAN.
- **Routeur** : Pas de connexion internet sur le routeur (réglé rapidement).

8.3 Team Building - Pizza Party

Ce mardi, afin de consolider les relations et l'entente au sein de l'équipe, nous avons décidé d'organiser un déjeuner commun et avons dégusté un repas convivial.

8.4 16h30 | Réunion du soir : Résumé de la journée

Cette réunion avait pour but d'établir un état de l'avancement du projet et de définir les futurs objectifs.

Objectifs accomplis

- Création d'une Base de Données (DB) fonctionnelle.
- Création de l'Active Directory et préparation de LDAP.
- Installation d'un système de monitoring (Zabbix), fonctionnel.
- Installation des règles firewall.
- Installation VPN (OpenVPN).
- Configuration initiale du switch L3.
- Création de multiples VMs.

Collaboration (Groupe C)

Les deux groupes sont très similaires au niveau de l'avancement.

Cependant, là où notre groupe (Groupe D) a du retard par rapport au groupe C (VPN, config physique, Backend), nous sommes par contre plus avancés au niveau de l'Active Directory, de la création des VMs et des hyperviseurs ainsi qu'au niveau du monitoring.

Nous collaborons afin de pallier à nos retards respectifs. L'objectif d'installer un VPN joignant les deux sites (IPsec) pour mercredi après-midi est toujours de mise.

8.5 Résumé de la journée en quelques photos

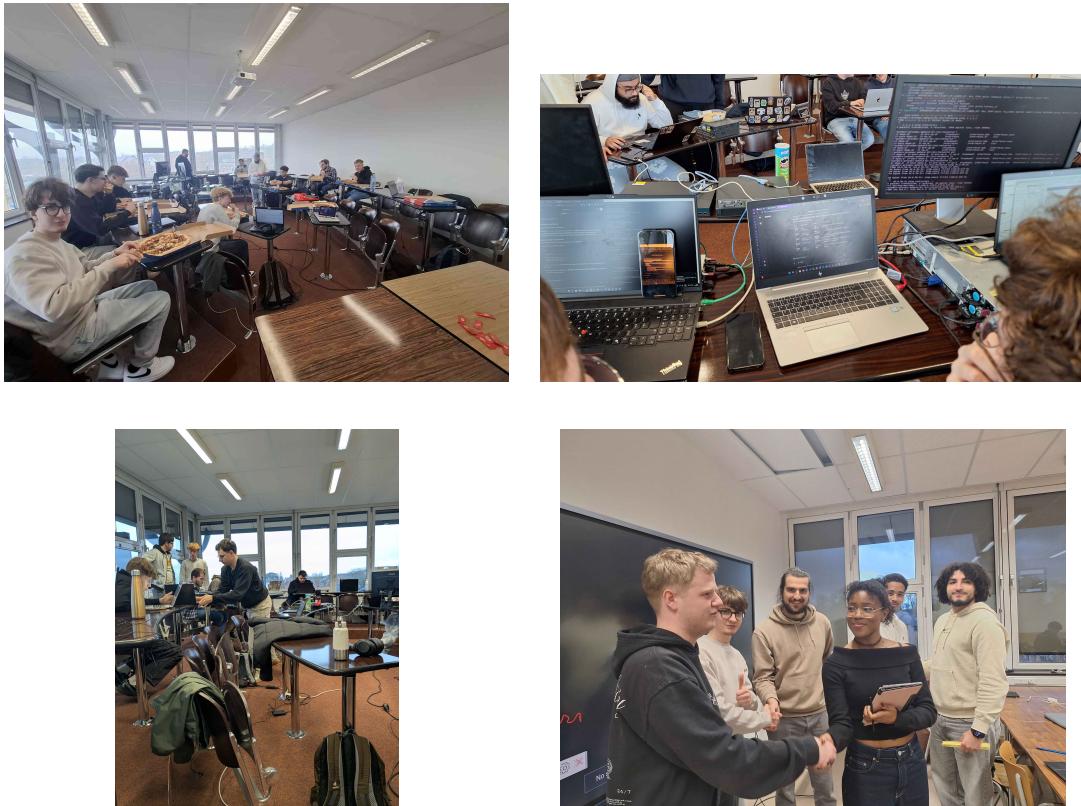


FIGURE 3 – Team Building et Avancement technique

9 Journal de Bord : Mercredi 04

9.1 09h00 | Réunion du matin : Organisation

Mise au point de l'avancement du travail, établissement des objectifs journaliers et répartition des tâches.

Objectifs journaliers

- Égaliser la RAM des serveurs.
- Connexions L3.
- Création des différents VLANs.
- Création des interfaces de Management (MGM).
- Fusionner le côté Auth/LDAP et la partie DB et connecter le tout à l'Active Directory.
- Effectuer le Frontend.
- Mettre en place les sécurités sur les appareils (ARP spoofing, etc.).
- VPN inter-groupe avec le groupe C.

Questions soulevées

- Quid du VPN inter-groupe ?

Problèmes rencontrés

- Pas de connexion internet depuis le L3.
- Pas de connexion internet depuis le firewall.

9.2 16h00 | Réunion du soir : Résumé de la journée

Cette réunion avait pour but d'établir un état de l'avancement du projet et de définir les futurs objectifs.

Objectifs accomplis

- Connexion du switch L3 à internet réussie.
- Finalisation du premier firewall.
- Création des interfaces de Management.
- Avancement significatif du Frontend.
- Fusion de l'Authentification/LDAP à la DB.
- Crédit de routes pfSense pour le VLAN 90 (correction du problème de connexion internet).

Prochains objectifs

- Configurer le second firewall.
- Installer et configurer les systèmes de monitoring.
- Configurer l'Active Directory.
- Installer les sécurités sur les différents appareils.
- Procéder à une vérification complète et minutieuse de l'ensemble du réseau.
- Terminer et déployer le site web.

Collaboration (Groupe C)

Après discussion avec le second groupe, nous nous sommes rendu compte que plusieurs facteurs retarderaient fortement, si ce n'est empêcheraient complètement l'installation du tunnel VPN.

- **Du côté du groupe C :** Un retard considérable et de nombreux problèmes techniques liés à une erreur d'adressage.
- **Du côté du groupe D :** Une difficulté jugée trop importante pour se permettre d'assigner un ou plusieurs membres sur l'installation du VPN au vu des délais.

9.3 Résumé de la journée en quelques photos

10 Journal de Bord : Jeudi 05 (En cours)

10.1 09h00 | Réunion du matin : Organisation

Mise au point de l'avancement du travail, établissement des objectifs journaliers et répartition des tâches.

Objectifs journaliers

- Configurer le deuxième firewall.
- Configurer l'Active Directory.
- Configurer les sécurités.
- Configurer les systèmes de monitoring.

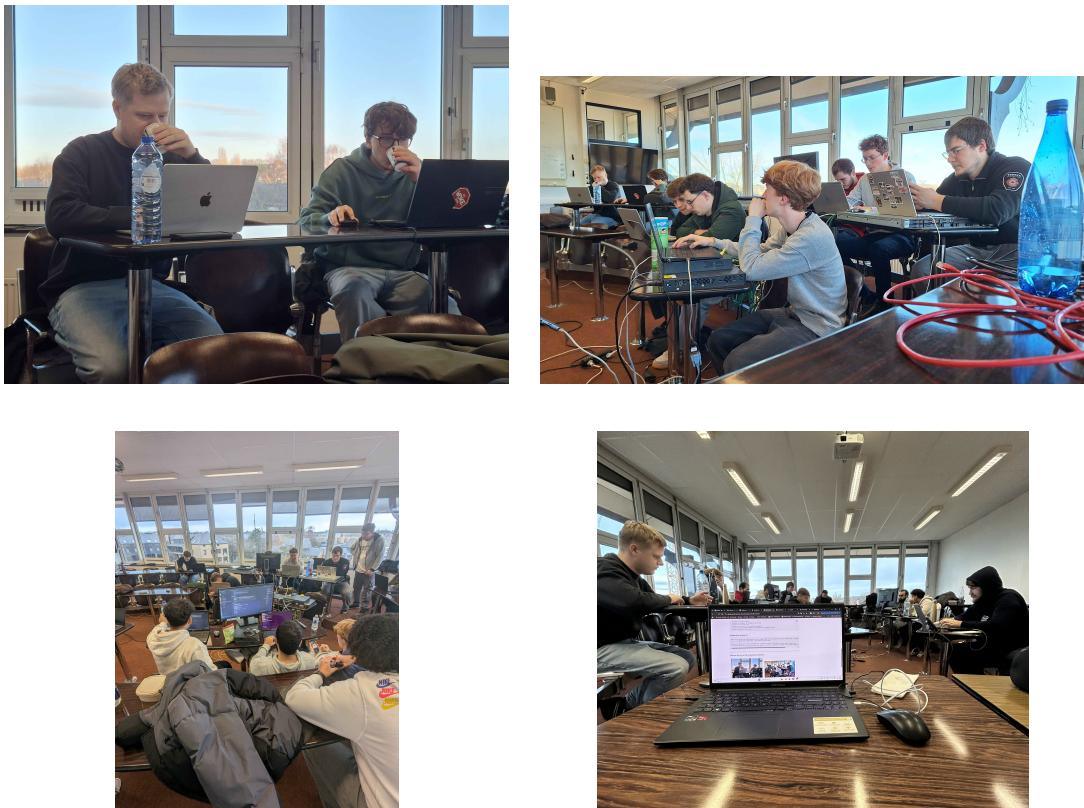


FIGURE 4 – Avancement technique et câblage

- Checking des connectivités.

Problèmes rencontrés

- Pas de connexion avec les agents Zabbix
- Pas de connexion internet sur l'AD
- VPN intersites non fonctionnel
- VPN client-side non fonctionnel
- FW2 non connecté

10.2 [16H30] | Réunion du soir : Résumé de la journée

Cette réunion avait pour but d'établir un état de l'avancement du projet et de définir les futurs objectifs.

Objectifs accomplis

- FW2 fonctionnel
- FW1 fonctionnel
- Site déployé
- Active Directory fonctionnel
- Monitoring installé (Zabbix, Loki, Backup)
- Sécurité switch L2
- Sécurité switch L3

10.3 Résumé de la journée en quelques photos

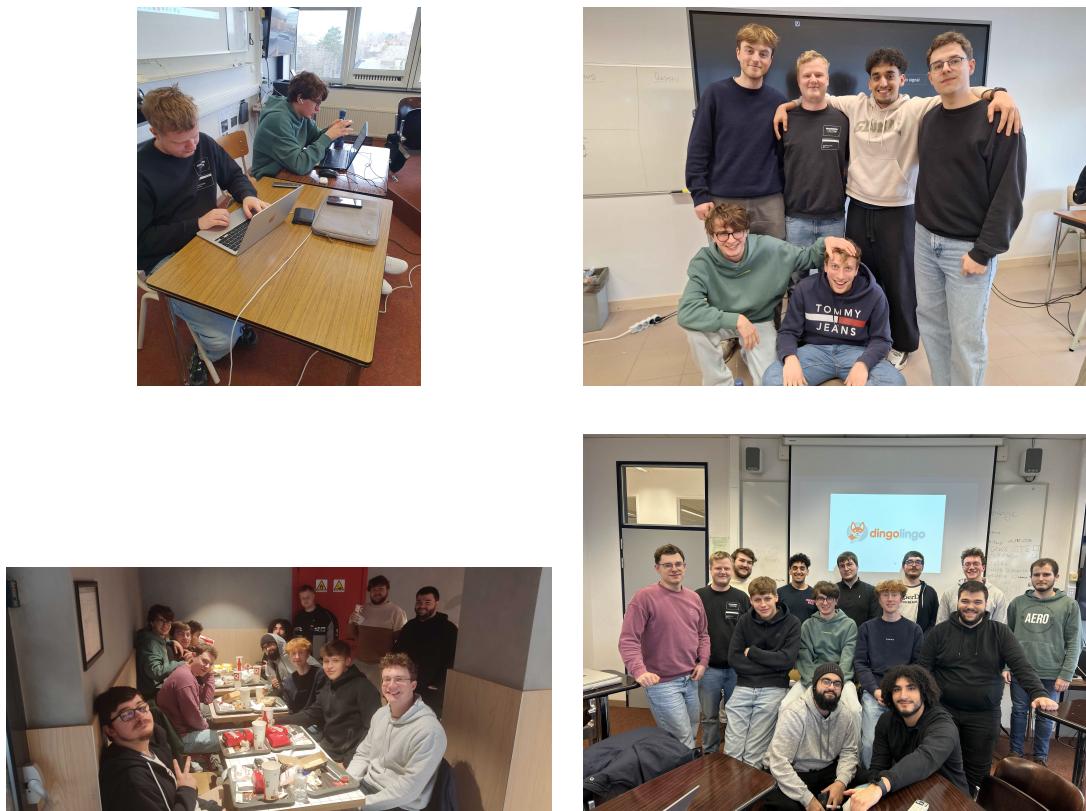


FIGURE 5 – Avancement du Jeudi

11 Topologie et plan d'adressage

11.1 Topologie logique

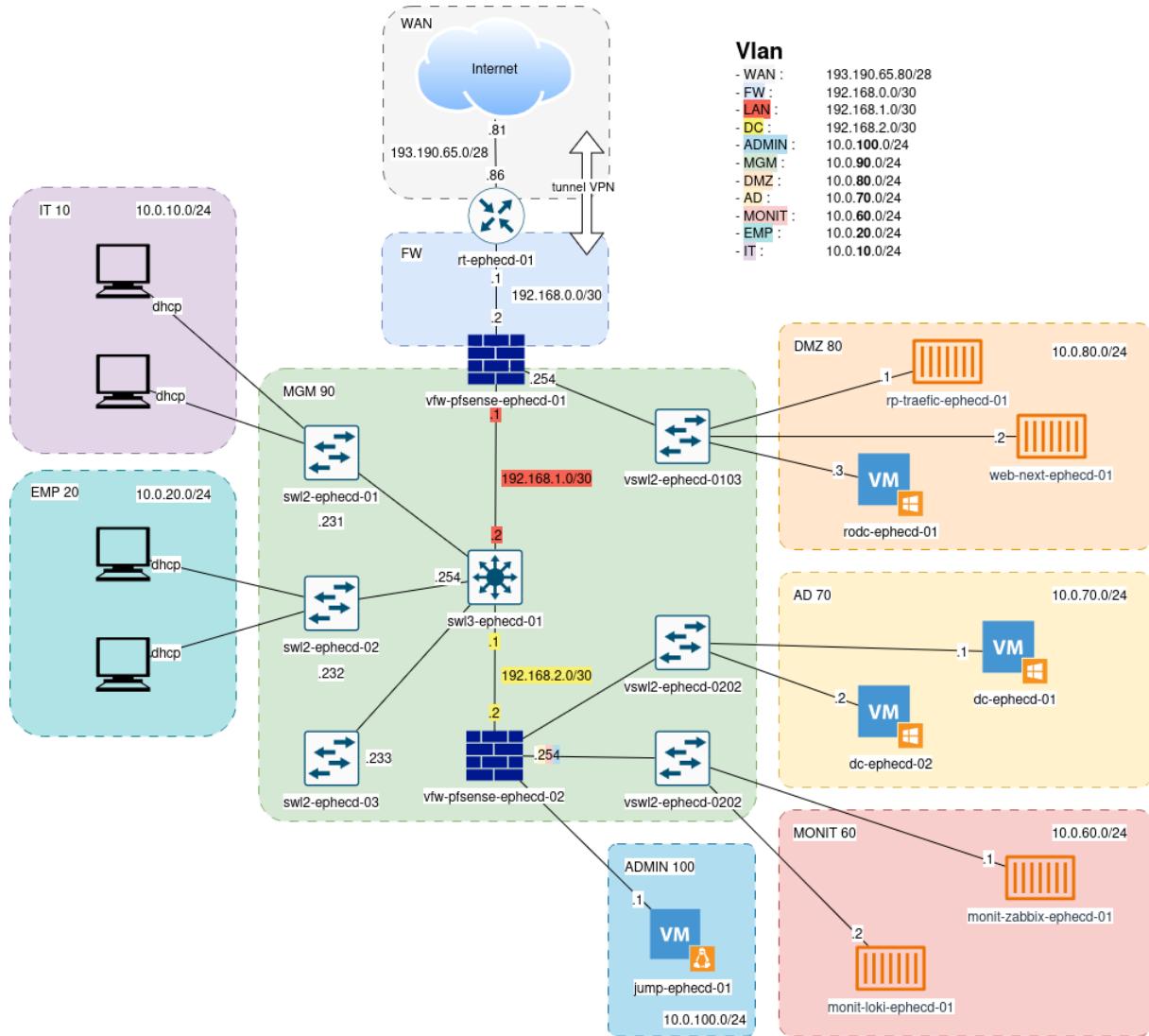


FIGURE 6 – Schéma de la topologie logique

11.2 VLAN et plans d'adressage

11.2.1 Tableau des VLAN

11.2.2 Adresses statiques

VLAN	Rôle	Réseau
WAN	Lien Internet	193.190.65.80/28
FW	Transit FW-L3	192.168.0.0/30
LAN	Transit L3-FW	192.168.2.0/30
ADMIN 100	Réseau admin / Jump	10.0.100.0/24
MGM 90	Management	10.0.90.0/24
DMZ 80	DMZ Web / Proxy	10.0.80.0/24
AD 70	Active Directory	10.0.70.0/24
MONIT 60	Monitoring	10.0.60.0/24
EMP 20	Clients employés	10.0.20.0/24
IT 10	Postes IT	10.0.10.0/24

TABLE 3 – Liste des VLANs et sous-réseaux

11.3 Topologie physique

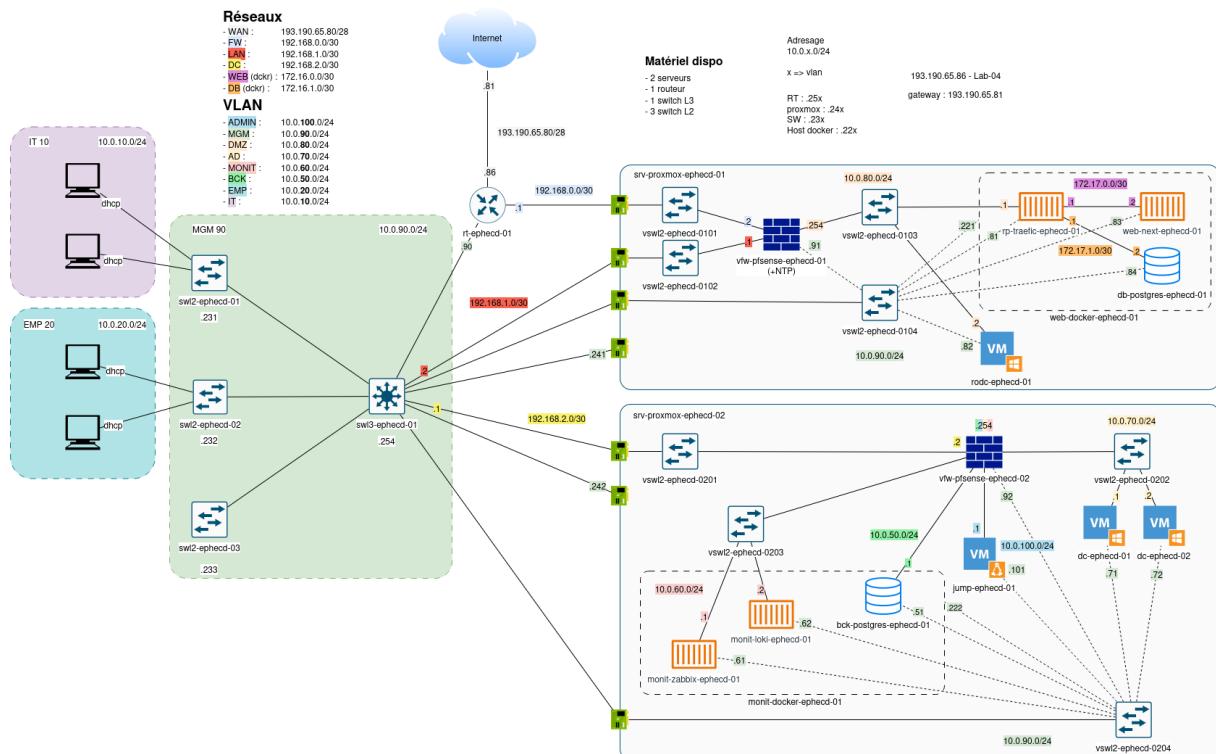


FIGURE 7 – Schéma de la topologie physique

Réseau / VLAN	Adresse IP	Équipement / Rôle
WAN	193.190.65.81	Passerelle Internet opérateur
WAN	193.190.65.86	Routeur r-ephecd-01
FW (Transit)	192.168.0.1	r-ephecd-01 (côté FW)
FW (Transit)	192.168.0.2	vfw-pfsense-ephecd-01
LAN (Transit)	192.168.2.1	swl3-ephecd-01 (SVI transit)
LAN (Transit)	192.168.2.2	vfw-pfsense-ephecd-02
MGM 90	10.0.90.254	swl3-ephecd-01 (Gateway VLAN 90)
MGM 90	10.0.90.231	swl2-ephecd-01
MGM 90	10.0.90.232	swl2-ephecd-02
MGM 90	10.0.90.233	swl2-ephecd-03
ADMIN 100	10.0.100.254	swl3-ephecd-01 (Gateway VLAN 100)
ADMIN 100	10.0.100.11	jump-ephecd-01
DMZ 80	10.0.80.254	swl3-ephecd-01 (Gateway VLAN 80)
DMZ 80	10.0.80.81	rp-traefic-ephecd-01
AD 70	10.0.70.254	swl3-ephecd-01 (Gateway VLAN 70)
AD 70	10.0.70.71	dc-ephecd-01
AD 70	10.0.70.72	dc-ephecd-02
MONIT 60	10.0.60.254	swl3-ephecd-01 (Gateway VLAN 60)
MONIT 60	10.0.60.61	monit-zabbix-ephecd-01
MONIT 60	10.0.60.62	monit-loki-ephecd-01
EMP 20	10.0.20.254	swl3-ephecd-01 (Gateway VLAN 20)
IT 10	10.0.10.254	swl3-ephecd-01 (Gateway VLAN 10)

TABLE 4 – Plan d'adressage statique détaillé

Action	Proto	Source	Dest	Port	Description
Block	Any	RFC1918	Any	Any	AntiSpoofing (Bloquer IP privées)
Pass	TCP	Any	HOST_RP	443	NAT vers Reverse Proxy
Pass	UDP	PfSense	NTP_Serv	123	Synchro Horloge Officielle
Block	Any	Any	Any	Any	Règle par défaut

TABLE 5 – Règles de flux WAN

Action	Proto	Source	Dest	Port	Description
Pass	TCP/UDP	NET_IT/EMP	HOST_DC	Ports_AD	Auth Active Directory (RWDC)
Pass	UDP	NET_IT/EMP	PfSense	123	NTP (Heure)
Pass	TCP	NET_IT	HOST_LOKI	443	Envoi des logs vers Loki
Pass	TCP	NET_IT	HOST_ZABBIX	443	Monitoring Zabbix
Pass	Any	NET_EMP	!RFC1918	Any	Accès Internet (Sauf privés)
Pass	Any	NET_IT	NET_MGM/ADM...	Any	Accès IT aux ressources sensibles
Block	Any	NET_IT/EMP	Any	Any	Bloque l'accès par défaut

TABLE 6 – Règles de flux IT & EMP

12 Configuration Firewall & VPN

12.1 Flux théoriques

12.1.1 1. Interface : WAN

12.1.2 2. Interfaces : IT (VLAN 10) & EMP (VLAN 20)

Note Technique : Logique de l'accès Internet

Pourquoi cette syntaxe (!RFC1918) ?

- **Destination** : Nous sélectionnons l'alias RFC1918 (qui contient 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12).
- **Invert Match (!)** : Nous cochons la case "Invert" dans le champ destination.
- **Logique** : Le pare-feu comprend : "Si la destination n'est pas un de mes réseaux privés internes, alors c'est forcément Internet. J'autorise."

12.1.3 3. Interface : DMZ (VLAN 80)

Action	Proto	Source	Dest	Port	Description
Pass	TCP	HOST_RP	HOST_WEB	443	Reverse Proxy vers Web Server
Pass	TCP	HOST_WEB	HOST_DB	3306/5432	Web Server vers Base de Données
Pass	TCP/UDP	HOST_WEB	HOST_RODC	Ports_AD	Web Server vers Auth RODC
Pass	TCP	NET_DMZ	HOST_LOKI	443	Logs DMZ vers Loki
Pass	TCP	NET_DMZ	HOST_ZABBIX	443	Monitoring Zabbix
Block	Any	NET_DMZ	Any	Any	Bloque l'accès par défaut

TABLE 7 – Règles de flux DMZ

Action	Proto	Source	Dest	Port	Description
Pass	TCP	HOST_ZABBIX	NET_MGM	10050	Zabbix poll vers agents
Pass	UDP	HOST_ZABBIX	NET_MGM	161	SNMP vers infrastructure

TABLE 8 – Règles de flux Monitoring

12.1.4 4. Interface : MONIT (VLAN 60)**12.1.5 5. Interface : AD (VLAN 70)**

Action	Proto	Source	Dest	Port	Description
Pass	TCP/UDP	HOST_DC	HOST_RODC	Ports_AD	RéPLICATION AD vers RODC
Pass	TCP	HOST_DC	HOST_LOKI	3100	Logs vers Loki
Pass	UDP	HOST_DC	PfSense	123	Récupération NTP

TABLE 9 – Règles de flux Active Directory

12.1.6 6. Interface : ADMIN (VLAN 100)

Action	Proto	Source	Dest	Port	Description
Pass	TCP	HOST_JUMP	RFC1918	22, 3389	Admin SSH/RDP vers infra
Pass	TCP	HOST_JUMP	HOST_ZABBIX	80/443	Accès Web Zabbix
Pass	TCP	HOST_JUMP	HOST_LOKI	3000	Accès Grafana
Pass	Any	NET_ADMIN	Any	Any	Accès complet Internet

TABLE 10 – Règles de flux Admin

12.2 Règles implémentées (Captures d'écran)

Interface WAN

Floating	WAN	MGM	AD	BACKUP	MONIT	JUMP					
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
NTP											
<input type="checkbox"/>		0/0 B	IPv4 UDP	192.168.2.2	*	192.168.1.1	123 (NTP)	*	none	Synchro NTP vers FW-Haut	
AD/DC											
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	IT_EMP	*	HOST_DC	88	*	none	Authentification Active Directory	
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	IT_EMP	*	HOST_DC	636 (LDAP/S)	*	none	Accès à l'annuaire	
<input type="checkbox"/>		0/0 B	IPv4 TCP	IT_EMP	*	HOST_DC	445 (MS DS)	*	none	Accès fichiers et SYSVOL (GPO)	
<input type="checkbox"/>		0/0 B	IPv4 TCP	IT_EMP	*	HOST_DC	3269	*	none	Global Catalog SSL	
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	IT_EMP	*	HOST_DC	464	*	none	Kerberos Password Change	
Monitoring											
<input type="checkbox"/>		0/0 B	IPv4 TCP	IT_EMP_DMZ	*	HOST_ZABBIX	Ports_ZABBIX	*	none	Monitoring Zabbix	
<input type="checkbox"/>		0/0 B	IPv4 TCP	IT_EMP_DMZ	*	HOST_LOKI	Ports_LOKI	*	none	Envoi des logs vers Loki	
Block par défaut											
<input type="checkbox"/>		0/0 B	IPv4 *	*	*	*	*	*	none	Règle implicite par défaut	

FIGURE 8 – Règles WAN

Interface LAN

NTP											
<input type="checkbox"/>		0/0 B	IPv4 UDP	IT_EMP	*	PfSense	123 (NTP)	*	none	NTP (Heure)	
<input type="checkbox"/>		0/0 B	IPv4 UDP	HOST_DC	*	PfSense	123 (NTP)	*	none	Récupération NTP des DC	
<input type="checkbox"/>		0/0 B	IPv4 UDP	192.168.2.2	*	PfSense	123 (NTP)	*	none	NTP pour FW-Bas	
Accès importants											
<input type="checkbox"/>		0/0 B	IPv4 *	NET_EMP	*	! RFC1918	*	*	none	Accès Internet (Tout sauf réseaux privés)	
<input type="checkbox"/>		0/0 B	IPv4 *	NET_IT	*	MGM_DMZ	*	*	none	Accès IT aux VLAN MGM et DMZ	
AD/RODC											
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	HOST_DC	*	HOST_RODC	88	*	none	Réplication AD vers RODC	
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	HOST_DC	*	HOST_RODC	636 (LDAP/S)	*	none	Réplication AD vers RODC	
<input type="checkbox"/>		0/0 B	IPv4 TCP	HOST_DC	*	HOST_RODC	445 (MS DS)	*	none	Réplication AD vers RODC	
<input type="checkbox"/>		0/0 B	IPv4 TCP	HOST_DC	*	HOST_RODC	3269	*	none	Réplication AD vers RODC	
<input type="checkbox"/>		0/0 B	IPv4 TCP/UDP	HOST_DC	*	HOST_RODC	464	*	none	Réplication AD vers RODC	
Accès ADMIN											
<input type="checkbox"/>		0/0 B	IPv4 *	NET_ADMIN	*	*	*	*	none	Accès complet	
DB											
<input type="checkbox"/>		0/0 B	IPv4 TCP	HOST_DB_BACK	*	HOST_DB	5432	*	none	Récupération des données DB	
Bloque Accès											
<input type="checkbox"/>		0/0 B	IPv4 *	IT_EMP	*	*	*	*	none	Bloque l'accès par défaut	

FIGURE 9 – Règles LAN (Global et suite)

Interface DMZ

Monitoring											
<input type="checkbox"/>		0/0 B	IPv4 TCP	NET_DMZ	*	HOST_LOKI	Ports_LOKI	*	none	Logs DMZ vers Loki	
<input type="checkbox"/>		0/0 B	IPv4 TCP	NET_DMZ	*	HOST_ZABBIX	Ports_ZABBIX	*	none	Monitoring Zabbix	
Bloque Accès											
<input type="checkbox"/>		0/0 B	IPv4 *	NET_DMZ	*	*	*	*	none	Bloque par défaut	

FIGURE 10 – Règles DMZ

Interface AD (Active Directory)

AD/DC											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP	HOST_DC	*	HOST_RODC	88	*	none	RéPLICATION AD VERS RODC	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP	HOST_DC	*	HOST_RODC	636 (LDAP/S)	*	none	RéPLICATION AD VERS RODC	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	HOST_DC	*	HOST_RODC	445 (MS DS)	*	none	RéPLICATION AD VERS RODC	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	HOST_DC	*	HOST_RODC	3269	*	none	RéPLICATION AD VERS RODC	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP	HOST_DC	*	HOST_RODC	464	*	none	RéPLICATION AD VERS RODC	
NTP											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 UDP	HOST_DC	*	192.168.1.1	123 (NTP)	*	none	RÉCEPTION NTP DES DC	
Monitoring											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	HOST_DC	*	HOST_LOKI	Ports_LOKI	*	none	ENVOI DES LOGS VERS LOKI	

FIGURE 11 – Règles Active Directory

Interface MGM (Management)

Mangement											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/UDP	NET_MGM	*	RFC1918	Ports_MGM	*	none	ACCÈS DE MGM POUR LA GESTION	

FIGURE 12 – Règles Management

Interface MONIT (Monitoring)

Floating	WAN	MGM	AD	BACKUP	MONIT	JUMP					
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Monitoring											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	HOST_ZABBIX	*	RFC1918	10050	*	none	ZABBIX POLL VERS TOUS LES AGENTS	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 UDP	HOST_ZABBIX	*	RFC1918	161 (SNMP)	*	none	SNMP VERS INFRASTRUCTURE	

FIGURE 13 – Règles Monitoring

Interface BCK (Backup)

Floating	WAN	MGM	AD	BACKUP	MONIT	JUMP					
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
DB											
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	HOST_DB_BACK	*	HOST_DB	5432	*	none	RÉCEPTION DES DONNÉES DB	

FIGURE 14 – Règles Backup

13 Sécurité

Cette page décrit l'ensemble des mesures de sécurité mises en place sur les appareils du réseau.

14 Sécurisation des Commutateurs (Switching)

La sécurité de la couche 2 (Liaison de données) est critique pour empêcher les attaques locales telles que le *Man-in-the-Middle*, le *Flooding* ou l'usurpation d'identité. Voici les mesures concrètes appliquées sur nos commutateurs Cisco.

14.1 Durcissement global et administratif

Afin d'éviter la lecture des mots de passe en clair dans les fichiers de configuration (par exemple via un `show run`), nous chiffrons tous les mots de passe système. De plus, nous limitons la découverte du réseau par des tiers en désactivant CDP sur les ports utilisateurs.

- **Service Password Encryption** : Chiffre les mots de passe (type 7).
- **CDP (Cisco Discovery Protocol)** : Désactivé sur les ports d'accès pour ne pas divulguer d'informations sensibles (modèle, IP, version OS) aux utilisateurs finaux.

Listing 1 – Configuration de base

```
(config)# service password-encryption

! Désactivation de CDP sur les ports utilisateurs
(config)# interface range FastEthernet0/2-24
(config-if)# no cdp enable
(config-if)# exit

! Maintien de CDP uniquement sur les liens entre équipements (Uplink)
(config)# interface FastEthernet0/1
(config-if)# cdp enable
```

14.2 Protection contre les attaques DHCP (DHCP Snooping)

Le **DHCP Snooping** permet de lutter contre le *DHCP Flooding* (épuisement du pool d'adresses) et l'installation de serveurs DHCP pirates (*Rogue DHCP*).

- Le switch surveille les échanges DHCP.
- Seul le port **Uplink** (vers le routeur/serveur légitime) est "Trust" (de confiance). Les ports utilisateurs sont "Untrust" et ne peuvent pas envoyer d'offres DHCP (DHCPOFFER).
- La commande `no ip dhcp snooping information option` est ajoutée pour éviter les erreurs de rejet de paquets (Option 82) lors du relais vers le serveur.

Listing 2 – Mise en place du DHCP Snooping

```
! Activation globale
(config)# ip dhcp snooping
(config)# ip dhcp snooping vlan 10,90
(config)# no ip dhcp snooping information option

! Configuration du port de confiance (Vers Routeur/Serveur)
(config)# interface FastEthernet0/1
(config-if)# ip dhcp snooping trust
```

14.3 Protection contre l'ARP Poisoning (DAI)

L'**ARP Spoofing** (ou Cache Poisoning) permet à un attaquant de s'interposer dans les communications. Nous utilisons **Dynamic ARP Inspection (DAI)**.

- Le switch vérifie la conformité des paquets ARP par rapport à la base de données créée par le DHCP Snooping (liaison IP ↔ MAC).
- Les paquets ARP invalides sont rejetés.
- Un *rate-limit* est appliqué pour empêcher le *ARP Flooding* qui pourrait surcharger le CPU du switch.

Listing 3 – Configuration de Dynamic ARP Inspection

```
! Activation par VLAN
(config)# ip arp inspection vlan 10

! Le port Uplink ne doit pas être filtré
(config)# interface FastEthernet0/1
(config-if)# ip arp inspection trust

! Protection contre le flood ARP sur les ports utilisateurs
(config)# interface range FastEthernet0/2-24
(config-if)# ip arp inspection limit rate 15
```

14.4 Protection de l'architecture VLAN (DTP & Hopping)

Pour empêcher le *VLAN Hopping* (saut de VLAN) où un attaquant force la négociation d'un lien Trunk pour accéder à des réseaux restreints :

- Les ports utilisateurs sont forcés en mode **Access**.
- Le protocole DTP (*Dynamic Trunking Protocol*) est désactivé via `switchport nonegotiate`.

Listing 4 – Désactivation de la négociation DTP

```
! Configuration de l'Uplink (Trunk statique sans négociation)
(config)# interface FastEthernet0/1
(config-if)# description Uplink_Trunk
(config-if)# switchport mode trunk
(config-if)# switchport nonegotiate

! Verrouillage des ports utilisateurs
(config)# interface range FastEthernet0/2-24
(config-if)# switchport mode access
(config-if)# switchport nonegotiate
```

14.5 Protection STP et Port Security

Enfin, nous sécurisons la topologie réseau et l'accès physique.

1. STP Security :

- **BPDU Guard** : Si un utilisateur branche un switch non autorisé, le port se coupe immédiatement pour éviter les boucles.
- **Root Guard** : Empêche un équipement tiers de devenir le pont racine (*Root Bridge*) et de détourner le trafic.

2. Port Security : Limite le nombre d'adresses MAC sur un port pour empêcher le *MAC Flooding* (saturation de la table CAM).

Listing 5 – STP et Port Security

```
! Sécurisation Spanning-Tree
(config)# spanning-tree bpduguard enable
(config)# spanning-tree guard root

! Activation de la sécurité de port (Par défaut : Max 1 MAC)
(config)# interface range FastEthernet0/2-10
(config-if)# switchport port-security
```

14.6 Durcissement des équipements (Device Hardening)

- **Accès distant** : Configuration de SSHv2 uniquement (Telnet désactivé).
- **Authentification** : Mots de passe chiffrés (service password-encryption) et utilisateurs locaux sécurisés.
- **Bannières** : Mise en place de bannières d'avertissement (MOTD).

14.7 Sécurité de Niveau 2 (Switching)

- **Port Security** : Limitation du nombre d'adresses MAC par port.
- **DHCP Snooping** : Protection contre les serveurs DHCP non autorisés.
- **Dynamic ARP Inspection (DAI)** : Protection contre l'ARP Spoofing.
- [À compléter]

15 LDAP et Authentification

Cette section détaille le flux d'authentification en environnement de production.

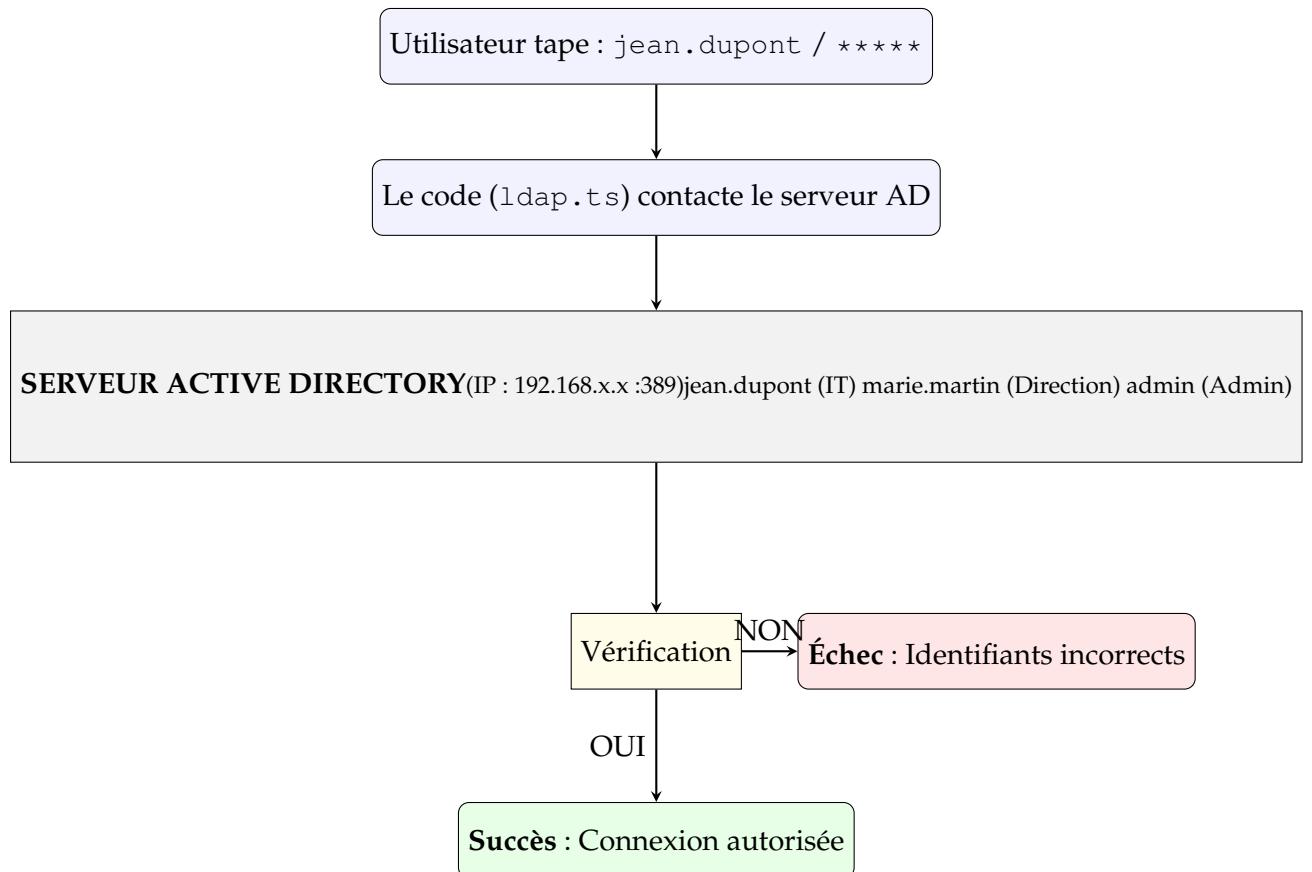


FIGURE 15 – Flux d'authentification LDAP en Production
(NEXT_PUBLIC_MOCK_AUTH="false")

15.1 Description du processus

Le schéma ci-dessus illustre le comportement de l'application lorsque le mode "Mock" est désactivé. L'application agit comme une passerelle qui interroge directement l'infrastructure Active Directory gérée par l'équipe Administration Système.

- **Sécurité :** Les mots de passe ne sont pas stockés dans l'application Web, mais vérifiés à la volée contre l'AD.
- **Rôles :** Les droits d'accès sont déterminés par les groupes d'appartenance de l'utilisateur dans l'Active Directory (IT, Direction, Admin).

16 Développement Web

16.1 Architecture Logicielle : Full-Stack Next.js & Prisma

Nous utilisons une stack moderne pour garantir performance et flexibilité.

- **Framework Web :** [Next.js](#)
- **ORM :** [Prisma](#) (avec Adapter PostgreSQL)
- **Base de Données :** PostgreSQL (Conteneurisé)
- **Style :** Tailwind CSS 4



FIGURE 16 – Stack Technique

16.2 1. Infrastructure & Virtualisation

L'environnement est entièrement conteneurisé pour assurer la parité entre le développement et la production sur le serveur final.

1. **Conteneur Web (`next.js_app`)** : Expose le service sur le port 3000, gère le rendu serveur (SSR) et les Server Actions.
2. **Conteneur DB (`postgres_db`)** : Base de données relationnelle persistante via un volume Docker.
3. **Gestion des Secrets** : Utilisation de fichiers `.env.local` exclus du tracking Git pour protéger les identifiants de la base de données et du LDAP.

16.3 2. Développement Backend & Base de Données

- **Modélisation (Schema Prisma)** : Mise en place d'une hiérarchie `Formation > Lesson > Exercise`.
- **Flexibilité** : Utilisation du type `JSONB` pour les options d'exercices, permettant de varier les types de questions (QCM, traduction, etc.).
- **Moteur de Quiz** : Développement du `QuizEngine`, un composant interactif avec barre de progression en temps réel et validation côté serveur.
- **Routage Dynamique** : Implémentation de routes `lessons/[id]` pour charger dynamiquement le contenu depuis PostgreSQL.

16.4 3. Sécurité & Authentification (LDAP)

L'accès à la plateforme est protégé et lié à l'infrastructure réseau de l'entreprise.

- **LDAP/AD** : Création d'un utilitaire de connexion pour lier les comptes utilisateurs au répertoire Active Directory.
- **Système de Mock** : Intégration d'un mode simulation permettant de tester le flux d'authentification sans serveur AD physique.
- **Audit** : Script `search_logs.sh` permettant de tracer les tentatives de connexion par IP et machine.

16.5 État du service LDAP

Bien que l'interconnexion avec l'Active Directory ne soit pas pleinement opérationnelle au moment de la remise (problème de connectivité infra), la couche applicative a été entièrement

développée et testée en environnement simulé. Le module est prêt pour le déploiement en production.

Implémentation de l'authentification (src/lib/ldap.ts)

```

// import ldap from 'ldapjs';

// D finir les r les
const ROLES = {
  STUDENT: 1,
  ADMIN: 2,
};

export const verifyLDAPCredentials = (username: string, password: string): Promise<any> => {
  return new Promise((resolve, reject) => {

    // 1. Mode simulation (MOCK) pour le d veloppement
    // Permet de valider le front-end sans d pendre de l'infra AD
    if (process.env.NEXT_PUBLIC_MOCK_AUTH === "true") {
      if (username === "admin" && password === "admin") {
        return resolve({
          displayName: "Admin de Test",
          mail: "admin@entreprise.be",
          isAdmin: true // Flag pour identifier l'admin
        });
      }
      // Utilisateur test normal
      if (password === "test") {
        return resolve({
          displayName: username,
          mail: `${username}@entreprise.be`,
          isAdmin: false
        });
      }
      return reject(new Error("Identifiants de test incorrects"));
    }

    // 2. Connexion r elle l'AD (Production)
    const client = ldap.createClient({ url: process.env.LDAP_URL! });
    const userDN = `cn=${username},${process.env.LDAP_BASE_DN}`;

    client.bind(userDN, password, (err) => {
      if (err) {
        client.unbind();
        return reject(err);
      }

      client.search(userDN, { scope: 'base' }, (err, res) => {
        if (err) {
          client.unbind();
          return reject(err);
        }

        res.on('searchEntry', (entry) => {
          // Extraction de l'objet utilisateur retour n par l'AD
          resolve((entry as any).object || (entry as any).pojo);
        });

        res.on('error', (err) => reject(err));
        res.on('end', () => client.unbind());
      });
    });
  };
}

export { ROLES };

```

16.6 4. Architecture du projet

Structure des fichiers (File Tree)

```
web_service/
    .env.example      <- Template
    .env.local        <- Secrets
    .gitignore        <- Protège les secrets
    docker-compose.yml <- Production avec Traefik
    docker-compose.dev.yml <- Développement local
    Dockerfile
    package.json
    prisma/
        schema.prisma
        seed.ts
    public/
        logo.png
    scripts/          <- Scripts bash utiles
    src/
        app/
            api/       <- APIs protégées
            admin/     <- Protection
            lessons/   <- Protection
            login/    <- Public
            ...
            components/
            lib/
                ldap.ts    <- Connexion AD
                prisma.ts
                session.ts
        middleware.ts   <- Security headers
    README.md
```

17 Reverse Proxy - Traefik

17.1 Objectif du reverse proxy

Nous utilisons **Traefik** comme reverse proxy HTTPS en frontal de notre application de formation en ligne. Ce composant est critique pour la sécurité et la scalabilité de l'infrastructure.

Il assure les fonctions suivantes :

- **Terminaison TLS** : Gestion automatique des certificats Let's Encrypt.
- **Redirection forcée** : Tout le trafic HTTP est redirigé vers HTTPS.
- **Routage intelligent** : Redirection du trafic vers le conteneur Next.js approprié.
- **Sécurité** : Injection d'en-têtes de sécurité HTTP supplémentaires.
- **Scalabilité** : Préparation au scaling horizontal (load balancing natif vers plusieurs instances).

17.2 Architecture globale

Le flux de données traverse les couches suivantes :

1. **Internet**
2. **Firewall** (pfSense / Routeur de bordure)
3. **Traefik** (Ports 80 et 443 exposés sur l'hôte)
4. **Réseau Docker web** (Zone interne)
5. **Conteneur app Next.js** (Port interne 3000)
6. **Réseau Docker internal**
7. **PostgreSQL** (Base de données isolée, non exposée)

Deux réseaux Docker distincts sont déclarés pour isoler la base de données du proxy public :

```
networks:
  web:
    external: false    # Communication Traefik <-> App
  internal:
    external: false    # Communication App <-> DB
```

17.3 Configuration de Traefik (Docker Compose)

Voici la configuration du service `traefik` dans notre fichier `docker-compose.yml` de production.

```
services:
  traefik:
    image: traefik:v3.0
    container_name: traefik
    env_file:
      - .env.local
    command:
      # Activation du Dashboard (s curis) et de l'API Docker
      - "--api.dashboard=true"
      - "--api.insecure=false"
      - "--providers.docker=true"
      - "--providers.docker.exposedbydefault=false"

      # Points d'entrée (Entrypoints)
      - "--entrypoints.web.address=:80"
      - "--entrypoints.websecure.address=:443"

      # Redirection automatique HTTP -> HTTPS
```

```

    - "--entrypoints.web.http.redirects.entryPoint.to=websecure"
    - "--entrypoints.web.http.redirects.entryPoint.scheme=https"

    # Configuration Let's Encrypt (ACME)
    - "--certificatesresolvers.letsencrypt.acme.tlschallenge=true"
    - "--certificatesresolvers.letsencrypt.acme.email=${ACME_EMAIL:-admin@example.com}"
    - "--certificatesresolvers.letsencrypt.acme.storage=/letsencrypt/acme.json"

    # Logging
    - "--log.level=INFO"
    - "--accesslog=true"

ports:
    - "80:80"
    - "443:443"

volumes:
    - /var/run/docker.sock:/var/run/docker.sock:ro # Accès au socket Docker
    - letsencrypt_data:/letsencrypt # Persistance des certificats

networks:
    - web
    - internal

labels:
    - "traefik.enable=false" # Le dashboard n'est pas exposé publiquement

restart: unless-stopped

```

Points clés de la configuration

- **Providers Docker**: L'option `exposedbydefault=false` nous oblige à activer explicitement Traefik sur chaque service via des labels, ce qui renforce la sécurité (pas d'exposition accidentelle).
- **Entrypoints** : Le port 80 (web) redirige systématiquement vers le port 443 (websecure).
- **Certificats** : Les certificats sont stockés dans un volume persistant (`acme.json`) et renouvelés automatiquement via le challenge TLS.
- **Sécurité du Dashboard** : Bien que l'API soit activée pour le monitoring interne, elle n'est pas exposée en mode "insecure".

17.4 Intégration de l'application Next.js

L'application Web est connectée à Traefik via des labels dynamiques.

```

app:
  build: .
  container_name: nextjs_app
  env_file:
    - .env.local
  environment:
    - NODE_ENV=production
  depends_on:
    - db
  networks:
    - web
    - internal
  labels:
    # Activation du routage pour ce conteneur
    - "traefik.enable=true"

    # Règle de routage basée sur le domaine
    - "traefik.http.routers.dingolingo.rule=Host('${DOMAIN:-localhost}')"
    - "traefik.http.routers.dingolingo.entrypoints=websecure"
    - "traefik.http.routers.dingolingo.tls.certresolver=letsencrypt"

```

```

# Port interne du conteneur
- "traefik.http.services.dingolingo.loadbalancer.server.port=3000"

# Application des Middlewares de sécurité
- "traefik.http.routers.dingolingo.middlewares=security-headers"
- "traefik.http.middlewares.security-headers.headers.frameDeny=true"
- "traefik.http.middlewares.security-headers.headers.contentTypeNosniff=true"
- "traefik.http.middlewares.security-headers.headers.browserXssFilter=true"
- "traefik.http.middlewares.security-headers.headers.stsSeconds=31536000"
- "traefik.http.middlewares.security-headers.headers.stsIncludeSubdomains=true"
  "

restart: unless-stopped

```

17.4.1 Routage et Middlewares de Sécurité

Le routeur dingolingo intercepte les requêtes destinées au nom de domaine configuré. Il applique ensuite une série de transformations via le middleware `security-headers` avant de transmettre la requête au port 3000 de l'application :

- **HSTS (Strict-Transport-Security)** : Force le navigateur à n'utiliser que HTTPS pendant 1 an (`max-age=31536000`).
- **Anti-Clickjacking** : `X-Frame-Options: DENY`.
- **Protection MIME** : `X-Content-Type-Options: nosniff`.
- **Filtre XSS** : Activation du filtre XSS du navigateur.

Ces en-têtes complètent la politique de sécurité de contenu (CSP) déjà gérée au niveau applicatif par Next.js.

17.5 Gestion des certificats et Environnements

17.5.1 Workflow Let's Encrypt

Dès la première requête HTTPS, Traefik initie un challenge TLS. Une fois validé par l'autorité de certification, le certificat est stocké localement. L'email de contact pour les notifications d'expiration est configuré via la variable d'environnement `ACME_EMAIL`.

17.5.2 Séparation Production / Développement

Nous maintenons une stricte séparation des configurations :

Production Utilisation de Traefik. Le port 3000 de l'application n'est **pas** exposé directement sur Internet, seul Traefik est accessible.

Développement Utilisation d'un fichier `docker-compose.dev.yml` simplifié sans Traefik pour faciliter le debugging.

docker-compose.dev.yml (Extrait)

```

services:
  app:
    build: .
    ports:
      - "3000:3000" # Exposition directe en dev uniquement
  environment:
    - NODE_ENV=development

```

17.6 Résumé des bénéfices

L'intégration de Traefik apporte trois avantages majeurs à notre architecture :

1. **Sécurité renforcée** : Surface d'attaque réduite (services internes masqués) et chiffrement de bout en bout forcé.
2. **Simplicité opérationnelle** : Configuration déclarative ("Infrastructure as Code") et gestion des certificats "zéro maintenance".
3. **Évolutivité** : Possibilité future d'ajouter d'autres services (ex : PgAdmin, Portainer) ou de multiplier les instances de l'application (Load Balancing) sans modifier l'architecture réseau externe.

18 Solution de Monitoring

Nous avons choisi **Zabbix** comme solution de monitoring centralisé pour assurer une surveillance proactive et en temps réel de l'ensemble des équipements et services de notre infrastructure.

18.1 Architecture retenue

Zabbix sera déployé selon une architecture client-serveur classique avec les composants suivants :

- **Serveur Zabbix** : Sera installé sur une **VM dédiée** (`monit-zabbix-ephecd-01`, VLAN 60 - 10.0.60.61) équipée de ressources suffisantes. Le serveur Zabbix assure la collecte des métriques, leur stockage en base MySQL/PostgreSQL et la génération des alertes.
- **Interface web Zabbix** : Accessible via le navigateur sur l'adresse <http://10.0.60.61/zabbix>, permettant la configuration des templates, la consultation des graphiques, la gestion des actions d'alerte et la supervision en temps réel de l'infrastructure.
- **Agents Zabbix** : Seront déployés sur **tous les serveurs physiques et virtuels** de l'infrastructure :
 - Hyperviseurs Proxmox (VLAN MGM 90)
 - Contrôleurs de domaine (VLAN AD 70)
 - Serveurs web et applications (VLAN DMZ 80)
 - Serveurs de monitoring complémentaires (VLAN MONIT 60)

18.2 Objets de monitoring

Zabbix collectera et supervisera les métriques réparties selon les catégories suivantes :

Métriques système

Utilisation CPU, mémoire, disque, swap ; Charge système et nombre de processus ; Espace disque et inodes disponibles.

Métriques réseau

Interfaces réseau (trafic in/out, erreurs, paquets) ; Latence ICMP vers équipements critiques ; Disponibilité des services réseau (HTTP, HTTPS, SSH, etc.).

Services applicatifs

État des services critiques (Apache, Nginx, MySQL, etc.) ; Temps de réponse applicatifs ; Nombre de connexions actives.

Spécificités infrastructure

Métriques Proxmox (VMs, stockage ZFS, tâches) ; RéPLICATION Active Directory ; Santé des services DNS/DHCP.

18.3 Objectifs fonctionnels

Cette solution de monitoring nous permettra de :

- **Superviser en temps réel** l'état de tous les équipements.
- **DéTECTER proactivEMENT** les baisses de performance avant impact utilisateur.
- **Recevoir des alertes immédiates** par email, Slack ou SMS en cas d'incident critique.
- **Analyser les tendances historiques** sur des périodes de plusieurs mois.
- **Automatiser la découverte** des nouveaux équipements (Low Level Discovery).
- **Inventorier automatiquement** la configuration matérielle/logicielle.

18.4 Avantages de cette solution

- **Support multi-plateforme** : Agents natifs Linux/Windows, SNMP pour équipements réseau.
- **Templates prêts à l'emploi** : Bibliothèque de 1000+ templates officiels.
- **Flexibilité des triggers** : Seuils adaptatifs, expressions mathématiques complexes.
- **Escalades intelligentes** : Gestion des alertes avec escalade et acknowledge.
- **API REST complète** : Intégration avec outils d'automatisation.
- **Dashboarding riche** : Graphiques, cartes réseau, SLA computation.

19 Solution de centralisation des logs

Nous avons opté pour **Grafana Loki** comme solution de centralisation des logs afin de conserver une trace complète et consultable de tous les événements se déroulant sur notre infrastructure.

19.1 Architecture retenue

Cette solution repose sur trois composants complémentaires déployés de manière distribuée :

Loki

Sera installé sur une **VM dédiée** (monit-loki-ephecd-01, VLAN 60 - 10.0.60.62) fonctionnant en conteneurs Docker. Loki constitue le moteur de stockage et d'indexation des logs, capable de gérer efficacement des volumes importants de données textuelles grâce à son indexation par labels.

Grafana

Sera hébergé sur la même VM Loki, offrant une interface web intuitive pour la consultation, la recherche et la visualisation des logs. Grafana permettra de créer des dashboards personnalisés, d'effectuer des recherches avancées via le langage **LogQL** et de configurer des alertes basées sur des patterns spécifiques.

Promtail

Sera déployé sous forme d'agent **sur chaque serveur et VM critique** de notre infrastructure (hyperviseurs Proxmox, contrôleurs de domaine, serveurs web, etc.). Promtail est responsable de la collecte en temps réel des fichiers de logs système (/var/log/*.log, journald, etc.), de leur étiquetage avec des métadonnées contextuelles (hostname, job, environnement) et de leur transmission vers Loki via le protocole HTTP natif (port 3100).

19.2 Objectifs fonctionnels

Cette architecture nous permettra de :

- **Centraliser l'ensemble des logs** d'une façon unifiée, indépendamment de leur source d'origine.
- **Déetecter rapidement les erreurs** et problèmes grâce à des requêtes LogQL ciblées.
- **Analyser les tendances** et corrélations entre événements sur différents systèmes.
- **Mettre en place des alertes proactives** sur des patterns critiques (ex : échecs d'authentification massifs, erreurs disque, etc.).
- **Préserver un historique configurable** (7 à 30 jours selon contraintes de stockage) pour les audits et analyses rétrospectives.

Monitoring

19.3 Avantages de cette solution

- **Faible empreinte** : Loki indexe uniquement les labels (clés/valeurs), pas le contenu des logs.
- **Scalabilité horizontale** : Facile d'ajouter des nœuds Loki ou Promtail.
- **Écosystème Grafana** : Intégration native avec Prometheus, Alertmanager et autres outils d'observabilité.
- **Support multi-format** : JSON, Syslog, journald, fichiers texte standards.

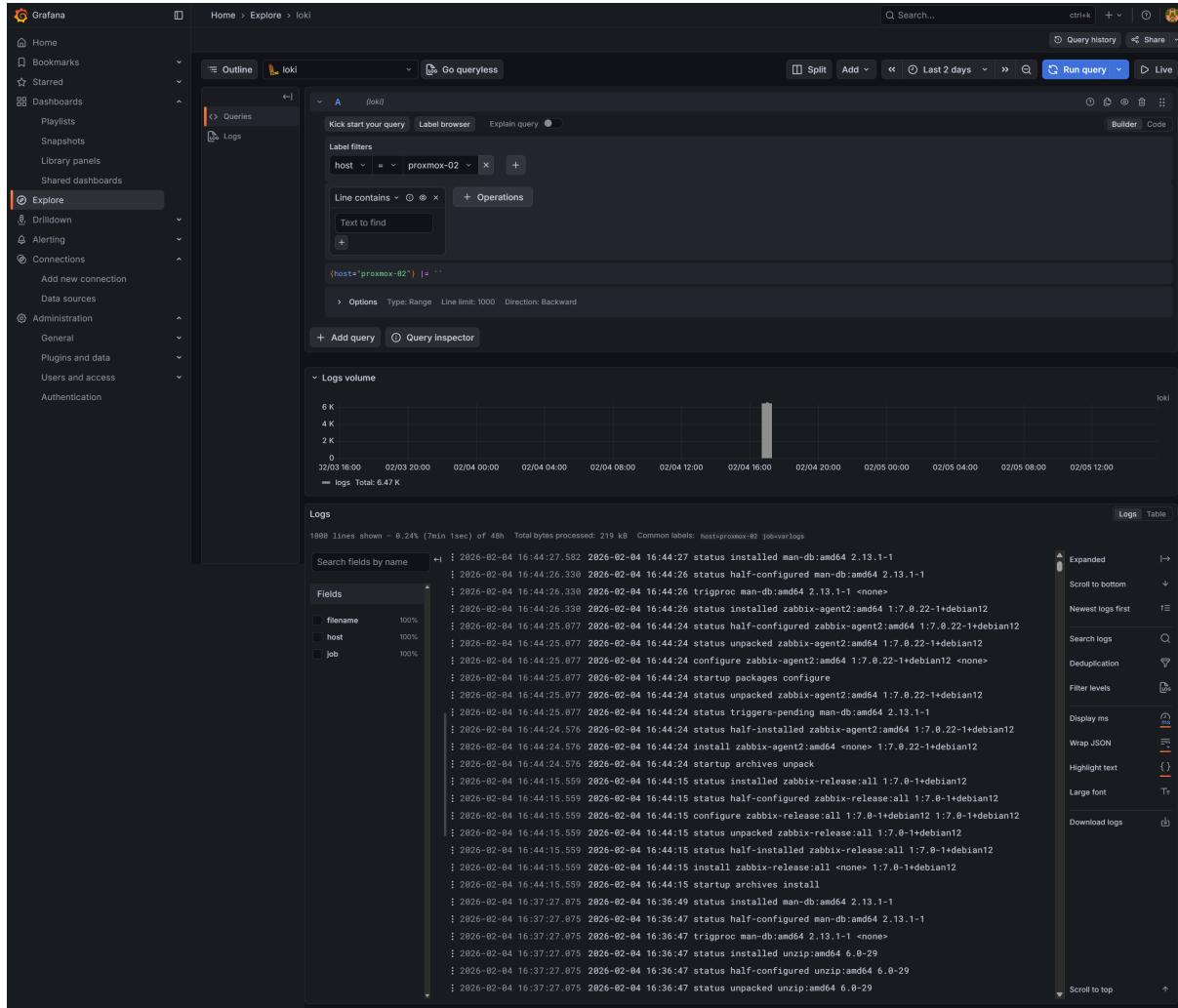


FIGURE 17 – Loki